IN THE CLAIMS:

1. - 6. (Cancelled)

7. (Original) A method for de-identification of records by and at a programmed client computer, comprising:

providing records to the programmed client computer;

locating personal identification data fields in each of the records;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected; and

one-way encrypting the personal identification data fields selected.

8. (Original) The method of claim 7 further comprising:

obtaining a mapping file; and

locating personal identification data fields in each of the records using the mapping file.

9. (Original) The method of claim 7 further comprising:

determining if the personal identification data fields selected are to be encoded; and

encoding the personal identification data fields to be encoded.

10. (Original) The method of claim 9 further comprising concatenating the personal identification data fields encoded with a seed value to provide seed value identifiers.

11. (Original) The method of claim 9 wherein the personal identification data fields are not concatenated with a seed value prior to the one-way encrypting.

12. (Original) The method of claim 7 wherein the one-way encrypting step comprises:

one-way encrypting with a first encryption algorithm the personal identification data fields selected to provide a first encryption result for each of the personal identification data fields selected; and

one-way encrypting with a second encryption algorithm the personal identification data fields selected to provide a second encryption result for each of the personal identification data fields selected.

13. (Original) The method of claim 12 wherein the one-way encrypting step comprises:

concatenating at least a portion of each of the first encryption result and the second encryption result for each of the personal identification data fields to respectively provide binary string identifiers for the personal identification data fields; and

converting the binary strings to alphanumeric strings to provide match codes.

14. (Original) A method for de-identification of records by a programmed client computer, comprising:

monitoring a file directory;

detecting presence of a new file in the file directory;

obtaining a mapping file for the new file;

locating personal identification data fields in records in the new file using the mapping file;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected;

determining if the personal identification data fields selected are to be encoded;

encoding the personal identification data fields to be encoded;

concatenating the personal identification data fields encoded with a seed value to provide seed value identifiers;

first one-way encrypting the seed value identifiers with a first encryption algorithm;

second one-way encrypting the seed value identifiers with a second encryption algorithm;

concatenating at least a portion of each one-way encryption result from the first one-way encrypting and the second one-way encrypting corresponding to the seed value identifiers to respectively provide binary strings for each of the seed value identifiers; and

converting the binary strings to alphanumeric strings to provide match codes;

wherein de-identified records comprising the match codes are created at the programmed client computer prior to transmission to a server computer.

15. - 22. (Cancelled)

23. (Original) A signal-bearing medium containing a program which, when executed by a programmed client computer, causes execution of a method comprising:

providing records to the programmed client computer;

locating personal identification data fields in each of the records;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected; and

one-way encrypting the personal identification data fields selected.

24. (Original) A signal-bearing medium containing a program which, when executed by a programmed client computer, causes execution of a method comprising:

monitoring a file directory;

detecting presence of a new file in the file directory;

obtaining a mapping file for the new file;

locating personal identification data fields in records in the new file using the mapping file;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected;

determining if the personal identification data fields selected are to be encoded;

encoding the personal identification data fields to be encoded;

concatenating the personal identification data fields encoded with a seed value to provide seed value identifiers;

first one-way encrypting the seed value identifiers with a first encryption algorithm;

second one-way encrypting the seed value identifiers with a second encryption algorithm;

concatenating at least a portion of each one-way encryption result from the first one-way encrypting and the second one-way encrypting corresponding to the seed value identifiers to respectively provide binary string for each of the seed value identifiers; and

converting the binary strings to alphanumeric strings to provide match codes;

wherein de-identified records comprising the match codes are created at the programmed client computer prior to transmission to a server computer.

25. (Original) The method of claim 24 wherein the programmed client computer comprises a mapper program, a parser program, a formatting program and an encoding program.

26. - 37. (Cancelled)

38. (New) A method for de-identification of records comprising:

locating personal identification data fields in a plurality of records;

parsing the personal identification data fields;

deleting a first portion of parsed said personal identification data fields; and

one-way encrypting a second portion of parsed said personal identification data fields to generate one or more de-identified records.

39. (New) The method of claim 38 further comprising:

selecting the second portion of parsed said personal identification data fields for one-way encryption.

40. (New) The method of claim 38 further comprising receiving the personal identification data fields with a client computer.

41. (New) The method of claim 38 further comprising providing the one or more de-identified records to a server computer.

42. (New) The method of claim 38 further comprising formatting be personal identification data fields prior to one-way encrypting a second portion of our said personal identification data fields.

43. (New) The method of claim 38 further comprising:

using a mapping file to locate the personal identification data fields in the plurality of records.

44. (New) The method of claim 38 further comprising:

determining the second portion of parsed said personal identification data fields to be one-way encrypted in response to deleting the first portion of parsed said personal identification data fields.

45. (New) The method of claim 44 further comprising concatenating the personal identification data fields that are one-way encrypted with a seed value to provide seed value identifiers.

46. (New) The method of claim 38 further comprising comparing the one or more de-identified records with one or more master records to determine linkage between the one or more de-identified records and de-one or more master records.

47. (New) A system for de-identifying records comprising:

a client computer having an interface for receiving records, wherein the client computer is adapted to locate personal identification data fields in the records, delete at least a portion of the personal identification data fields, and encrypt remaining personal identification data fields to generate encrypted personal identification data fields.

48. (New) The system of claim 47 further comprising a mapping file used to locate personal identification data fields in the records.

49. (New) The system of claim 47 wherein said at least a portion of the personal identification data fields are encoded with a seed value to provide seed value identifiers.

50. (New) The system of claim 47 wherein the encrypted personal identification data fields comprise one-way encryption with a first encryption algorithm to provide a first encryption result.

51. (New) The system of claim 50 wherein the encrypted personal identification data fields comprise one-way encryption with a second encryption algorithm to provide a second encryption result.

52. (New) The system of claim 51 wherein the one-way encryption with the first encryption result comprises concatenation of at least a portion of each of the first encryption result and the second encryption result for each of the personal identification data fields to respectively provide binary string identifiers for the personal identification data fields

53. (New) The system of claim 52 wherein the binary strings are converted to alphanumeric strings to provide match codes.

54. (New) A system for de-identification of records comprising:

means for locating personal identification data fields in a plurality of records;

means for parsing the personal identification data fields;

means for deleting a first portion of parsed said personal identification data fields; and

means for one-way encrypting a second portion of parsed said personal identification data fields to generate one or more de-identified records.